Exhibit 7

Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351 RJB UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, S. Kate Vaughan, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to Defendant's Motion to Suppress Evidence and Statements.

The defendant, Jay Michaud ("Michaud"), filed a motion to suppress evidence obtained via three court-authorized search warrants issued upon findings of probable cause by three neutral and detached magistrates, and of a Mirandized statement to law enforcement, alleging that the first of those search warrants was improperly issued. He does not challenge any of the assertions in any of the warrants. Rather, Michaud, a teacher with Vancouver Public Schools, contends that his use of a Tor-network-based child pornography website deprived any court of jurisdiction to issue a warrant to identify

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

him – an argument that, if accepted by this Court, could create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted site. Thankfully, his contention is wrong. The issuance of the challenged warrant complied with Fed. R. Crim. P. 41 and the Fourth Amendment, and was amply supported by probable cause to investigate the registered users of a massive child pornography website whose users, including Michaud, deployed advanced technological measures to hide their identity and location while they exploited children. Moreover, suppression would be particularly inappropriate here, where law enforcement officers acted reasonably and in good-faith reliance upon the issuance of warrants. Accordingly, for the reasons set forth more fully below, the United States requests that this Court deny the motion to suppress.

I. INTRODUCTION

The charges in this case arise from an investigation into a global online forum, referenced herein as "Website A," through which registered users like the defendant regularly advertised, distributed and accessed illegal child pornography.[1] The scale of child sexual exploitation on the site was massive –more than 150,000 total members collectively created and viewed tens of thousands of postings related to child pornography. Images and videos advertised, distributed and accessed through the site were highly categorized according to gender and age of victims portrayed – including "jailbait," "pre-teen" and "toddlers" – as well as the type of sexual activity depicted – including hardcore ("HC") and softcore ("SC"). The most postings (more than 20,000) occurred within a sub-section for "Pre-teen" videos dubbed "Girls HC," that contained hardcore pornographic images of pre-teen girls. The site also included forums for discussion of matters pertinent to child sexual abuse, including methods and tactics

[1] In order to protect the security of the ongoing investigation, the actual name of the website was not disclosed in pertinent search warrant documents, but was alternately referenced as the "TARGET WEBSITE" or "Website A." It is referenced herein as "Website A."

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

offenders use to abuse children and avoid law enforcement detection. It did not advertise or distribute adult pornographic images.

"Website A" operated on the anonymous Tor network. Use of the Tor network masks the user's actual Internet Protocol ("IP") address,[2] which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers. [3] To access the Tor network, a user must install Tor software by downloading an add-on to the user's web browser or the free "Tor browser bundle" available at www.torproject.org.[4] Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable. When a Tor user accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node.

Within the Tor network itself, entire websites, such as "Website A," can be set up as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of 16 algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client

---

[2] An Internet Protocol address or "IP" address refers to a unique number used by a computer to access the Internet. IP addresses are assigned to residential Internet users by an Internet Service Provider ("ISP").

[3] Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is publicly available at www.torproject.org. The Tor network is a haven for criminal activity in general, and the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited November 13, 2015).

[4] Users may also access Tor through so-called "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

and operating in the Tor network. Unlike an open Internet website, it is not possible use public lookups to determine the IP address of a computer hosting a "hidden service."

A "hidden service" like "Website A" is also more difficult for users to find. Even after connecting to the Tor network, a user must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find "Website A," a user had to first obtain the web address for it from another source – such as from other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing a Tor website like "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity taking place on "Website A," investigators faced a tremendous challenge to identify site users who were sexually exploiting children. Open-Internet, non-Tor websites generally have user IP address logs that can be used to locate and identify the site's users. In such cases, after the lawful seizure of a website whose users were engaging in unlawful activity, law enforcement could review IP logs and determine the IP addresses of site users. Agents could then determine from publicly-available information which Internet Service Provider ("ISP") owned an IP address, and issue a subpoena to that ISP to determine the user to which the IP address was assigned at a pertinent date and time. However, because "Website A" was a Tor "hidden service," any such IP logs would contain only the IP address of the last computer through which a user communication was routed. That last computer is not that of the actual user who sent the communication, and it is not possible to trace such communications back through the Tor network to that user. Such IP address logs therefore could not be used to locate and identify users of "Website A." Accordingly, in order for law enforcement to attain the sort of information that would normally be available from public sources and through ordinary investigative

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined that the computer server that hosted "Website A" was located at a web-hosting facility in North Carolina. In February of 2015, FBI agents apprehended the administrator of "Website A" and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of the site to go unidentified (and un-apprehended), the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia ("EDVA") during a brief two-week period between February 20, 2015, and March 4, 2015. During that brief period, the FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor site users' communications and (2) deploy a Network Investigative Technique ("NIT") on the site, in order to attempt to identify registered site users who were anonymously engaging in sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[5]

As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer instructions which, when downloaded (along with the other content of "Website A") by a registered user's computer, were designed to cause the user's computer to transmit a limited set of information – the computer's actual IP address and other computer-related information – that would assist in identifying the computer used to access "Website A" and its user. Ex. 1, pp. 23-27, ¶¶ 31-37. The search warrant authorization permitted that minimally-invasive technique to be deployed after a registered user logged into "Website A," which was located in EDVA, by entering a username and password. *Id.*, p. 24, ¶ 32; p. 23, Att. A.[6] IP address information

---

[5] The NIT search warrant, application, affidavit and return (No. 15-SW-89) are attached as Exhibit 1. The separate Title III application, affidavit and order are attached as Exhibit 5.

[6] The NIT affidavit explained that, in order to ensure technical feasibility and avoid detection of the technique by subjects of investigation, the FBI would deploy the technique more discretely against particular users, such as those

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

collected by the NIT, along with logs of activity on "Website A," was then used with further legal process to investigate "Website A" users.

At various points in his motion, Michaud, absent any factual or legal support or argument, inaccurately labels the government's court-authorized investigative technique as a "hacking." Mot. At 1, 8, 10. That is not the case. Even by dictionary definition, to hack involves gaining "unauthorized access to data" in a computer.[7] The federal statute under which what is colloquially known as computer hacking is commonly prosecuted – 18 U.S.C. § 1030 – criminalizes only the "unauthorized access" to a computer in certain defined circumstances and with particular stated intent. *Id*. The NIT, on the other hand, was a court-authorized investigative technique, whose deployment was supported by a showing of probable cause, that consisted of computer instructions designed only to cause the user's computer to transmit a limited set of information that would assist in identifying the computer used to access "Website A" and its user. Ex. 1, pp. 23-27, ¶¶ 31-37. The court-authorized NIT did not constitute "hacking" any more than a court-authorized search of a defendant's home, during which law enforcement seizes and removes evidence of a crime, constitutes burglary or theft. Michaud's use of such a loaded (and inaccurate) term is an obvious attempt to distract this Court's attention from the actual legal issues presented and invite a decision based upon something other than the pertinent facts and law. This Court should attach no weight to it whatsoever.

On July 9, 2015, law enforcement agents obtained from this District (Mag. J. David W. Christel) a search warrant for the defendant's home.[8] The warrant described "Website A" in detail and articulated that data obtained from logs on "Website A," court-authorized monitoring by law enforcement, and the court-authorized deployment of a NIT, had revealed that "Website A" user "Pewter" registered an account on "Website A"

---

who attained a higher status on the website by engaging in substantial activity, or in particular areas of the website, such as those with the most egregious examples of child pornography, which sub-forums were described in the affidavit. Ex. 1, pp 24-25, ¶ 32, n. 8.

[7] *See* Oxford Dictionaries Online, available at: http://www.oxforddictionaries.com/definition/english/hack (last visited November 16, 2015).

[8] The residential search warrant, application, and affidavit (No. 15-MJ-5111) are attached as Exhibit 2.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

on October 31, 2014 and spent 99 hours logged into the website between October 31, 2014, and March 2, 2015. Ex. 1, pp. 21-22, ¶¶ 25-26. Between February 20, 2015, and March 4, 2015, user "Pewter" viewed 187 message threads on the website, including threads with titles such as "10yo teen with anal front with his father," "Alicia 10 yo little girl loves adult sex (cum in mouth)," "7yo APRIL hj bj finger pencil in ass vib cum," "Lauri ~8yo 3 videos, tasting cum," and "Girl 12ish eats other girls/dirty talk." *Id.*, p. 22, ¶¶ 27-30. The warrant affidavit described specific child pornography "Pewter" accessed on March 2, 2015, which contained links to an image that depicted a prepubescent female being anally penetrated by the erect penis of an adult male. *Id.*, p. 23, ¶¶ 32-33. On February 28, 2015, user "Pewter," operating from IP address 73.164.163.63, accessed the post entitled "Girl 12ish eats other girls/dirty talk" in the section "Pre-teen Videos >> Girls HC." *Id.*, p. 22, ¶ 30. Information furnished by Comcast in response to an FBI subpoena tied the IP address collected by the NIT for "Pewter" to the Internet connection subscribed in his name at Michaud's then home. *Id.*, p. 23, ¶ 36. Further investigation determined that Michaud moved, as of May of 2015, to a new address that was the subject of the residential search warrant. *Id.*, pp. 23-26, ¶¶ 36-43.

On July 10, 2015, law enforcement officers executed a federal search warrant at Michaud's residence in Vancouver, WA. Agents located a thumb drive that was later determined to contain over 2,400 images of child pornography, including those depicting the anal rape of an infant and a toddler-aged child, and a 20-page manual entitled "The Jazz Guide: How to Have Sex With Very Young Girls . . . Safely." Ex. 4, p. 9, ¶ 31. Also on July 10, 2015, the defendant gave a brief, audio-recorded statement to law enforcement agents after being advised of his Miranda rights. He admitted to living alone and provided a password to his phone. After the interview, Michaud was arrested and charged by complaint with possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and (b)(2). A cell phone on the defendant's person was seized incident to his July 10, 2015 arrest. On August 11, 2015, officers obtained from this District (Mag.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

J. Karen Strombom) a warrant to search that phone, on which additional child pornography was located.[9]

On July 23, 2015, Michaud was indicted for receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and (b)(2). On October 16, 2015, the defendant filed a motion to suppress the NIT warrant and all information seized pursuant to it, including evidence obtained via execution of the residential search warrant and the defendant's post-Miranda statement to law enforcement.[10]

II. ARGUMENT

Michaud raises two unpersuasive arguments in his motion: that the issuance of the NIT warrant violated Rule 41 and that the defendant was not properly provided notice. On those purported bases, Michaud contends that evidence seized pursuant to that warrant and any related fruits should be suppressed. His arguments are without merit.

A. Summary of Argument

Michaud's argument for suppression based on a purported violation of the geographic limitations of Rule 41 fails for multiple reasons. Consistent with Rule 41, the NIT warrant was issued by a neutral and detached magistrate in the district where the website operated during the period of authorization, into which registered users – including Michaud – communicated while accessing the website, and in which the NIT was deployed. The Title III order for Michaud's communications with "Website A" also provided authority to obtain Michaud's IP address. And even if neither the NIT warrant nor the Title III order had provided authority for use of the NIT, its use would have been justified based on exigent circumstances pertaining to the ongoing exploitation and abuse of children and suspect offenders' use of anonymizing technology. Michaud's argument regarding delayed notice also fails, because the issuing Court authorized and extended delayed notice and Michaud was provided notice within the Court-authorized time frame.

---

[9] The search warrant, application, and affidavit (No. 15-5136) are attached as Exhibit 3.

[10] The defendant's motion to suppress does not make reference to the warrant to search the cell phone or its fruits.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The NIT warrant further satisfies the Fourth Amendment because it was issued based on a detailed, 31-page affidavit that amply articulated probable cause to deploy the NIT to registered users of a website dedicated to the advertisement and distribution of child pornography, and which described with particularity exactly what information would be collected through the NIT – IP address and other computer-related information – and how that information would assist with identifying site users and computers used to access the site. The affidavit accordingly established a more than fair probability that evidence of a crime – *i.e.*, of the identity of perpetrators – would be found via issuance of the warrant.

In any event, while neither the asserted violation of Rule 41 nor any of the defendant's other arguments warrant suppression, law enforcement acted at all times in good-faith reliance upon warrants issued upon findings of probable cause by neutral and detached magistrates in two different U.S. Districts. The extreme remedy of suppression is not justified where, as here, law enforcement diligently sought and received judicial approval to deploy an investigative technique necessitated by suspects' use of anonymizing technology to criminally exploit children.

B. The Warrant was Issued Consistent With Rule 41 and the Fourth Amendment

Michaud makes no substantive argument that the NIT warrant did not comply with the Fourth Amendment. Instead, he argues for suppression based on a purported violation of the geographic limitations of Rule 41. His argument fails for multiple reasons. First, the NIT warrant was consistent with Rule 41. Second, the Title III order for Michaud's communications with "Website A" also provided authority to obtain his IP address. Third, if neither the NIT warrant nor the Title III order provided authority for the NIT, its use would be justified based on exigent circumstances. Finally, even if the NIT warrant did violate Rule 41, suppression is not an appropriate remedy.

It is important to make clear the ramifications of Michaud's Rule 41 argument. When the government sought the NIT warrant, Michaud and thousands of others were

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

using "Website A" to access and share child pornography. The site was designed to hide the identity and location of its users, so the government had no way to know where Michaud was without first using the NIT authorized by the warrant. Thus, Michaud does not argue that the government should have sought its warrant elsewhere, or that the government should have more scrupulously followed any of the procedures of Rule 41 for obtaining or executing the warrant. Instead, Michaud is arguing that his use of the Tor hidden service deprived any court of jurisdiction to issue a warrant to identify him. If Michaud were correct, use of a Tor hidden service could potentially create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted hidden service. Fortunately, Michaud is wrong.

Courts interpret Rule 41 broadly to allow searches consistent with the Fourth Amendment. For example, in *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at that time did not include information and that Rule 41 required that a search be conducted within 10 days. *See id.* at 169 & n.16. The Court held that Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause," and it bolstered its conclusion by reliance on Rule 57(b), which provided that "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *Id.* at 169-70.[11] Similarly, in *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992), the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. Moreover, as the Seventh Circuit recognized, denying courts the authority to issue warrants for searches consistent with the Fourth Amendment would encourage warrantless searches, as such searches could be justified

[11] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

based on exigency: "holding that federal courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment." *United States v. Torres*, 751 F.2d 875, 880 (1984) (upholding video surveillance warrant). Based on the reasoning of these cases, this Court should reject Michaud's argument that Rule 41 should be interpreted narrowly to prohibit the use of search warrants to investigate those who use Tor to hide the location of their criminal activities.

In any event, the government did not violate Rule 41. Rule 41(b) is flexible enough to allow the issuance of warrants to investigate Tor hidden services.[12] In fact, three separate provisions of Rule 41(b) support issuance of the NIT warrant.

First, Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the warrant authorized use of the NIT (a set of computer instructions) located on a server in EDVA when the warrant was issued. Ex. 1, pp. 22-23, 24 ¶¶ 30, 33. As Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information," the NIT constituted property located in EDVA when the warrant was issued. Moreover, the NIT was deployed only to registered users of "Website A" who logged into the website, located in EDVA, with a username and password. *Id.*, Att. A. Each of those users – including Michaud – accordingly reached into EDVA's jurisdiction

---

[12] In order to eliminate any ambiguity on this issue, the Advisory Committee on Criminal Rules has endorsed an amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." *See* Advisory Committee on Rules of Criminal Rules, May 2015 Agenda, at 107-08 (available at http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books). The proposed rule was approved by the Advisory Committee on the Criminal Rules in March 2015 and the Standing Committee in May 2015. It is now pending further review before the U.S. Judicial Conference. *See* http://www.uscourts.gov/rules-policies/pending-rules-amendments.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

to access the site (and the child pornography therein). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT outside of EDVA.

Similarly, Rule 41(b)(4) specifies that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install within the district a tracking device in a container holding contraband, and investigators might then determine the location of the container after targets of the investigation carry the container outside the district. In this case, the NIT functioned in a similar manner, except in the Internet context. Investigators installed the NIT in EDVA on the server that hosted "Website A." When Michaud logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information from Michaud's computer back to law enforcement. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate Michaud. Thus, even if Rule 41(b)(2) did not provide authority to issue the warrant, Rule 41(b)(4) did so.

Furthermore, the EDVA warrant was issued by a judge in the district with the strongest known connection to the search: Michaud retrieved the NIT from a server in EDVA, and the NIT sent his network information back to a server in that district. The magistrate judge had authority under Rule 41(b)(1) to authorize a search warrant for "property located within the district." In addition, Michaud's use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in. In this circumstance, it was reasonable for the EDVA magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the EDVA warrant does not risk significant abuse because, as with all warrants, the manner of execution "is subject to later judicial review as to its

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

Michaud cites a single magistrate judge's opinion holding that Rule 41(b) does not authorize issuance of a warrant for use of a different (and significantly more invasive) NIT than the one used in this case. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). But that court did not fully consider the arguments here for the issuance of the warrant, let alone the arguments why suppression would be inappropriate after such a warrant was issued by a neutral and detached magistrate. Furthermore, to the government's knowledge, in every other matter involving an application for a search warrant to identify a person hiding his identity and location using Internet anonymizing techniques, the judge has issued the warrant. *See, e.g., United States v. Cottom, et. al.*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #122, Attachment 1; Doc. #123, Attachment 1) (2 separate NIT search warrants), (Doc #155) (denying suppression motion); *In re Search of NIT for Email Address texas.slayer@yahoo.com*, No. 12-sw-5685 (D. Col. October 9, 2012) (Doc #1) (search warrants); *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government*, No. 07-mj-5114 (W.D. Wash. June 12, 2007), *available at* http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.

Moreover, the reasoning of the Texas magistrate judge's decision does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp. 2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply because there was no showing that the installation of the NIT software would be within its district. *See id*. That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the server in EDVA. As the analogy to physical tracking devices demonstrates, the government "installs" the NIT within the meaning of Rule 41(b)(4) when it adds the NIT

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

to computer code on a computer in the issuing court's district. Michaud's subsequent retrieval of the NIT and its collection of information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included "installation" on Michaud's computer.

The Rule 41 warrant is not the only court order providing authority to obtain Michaud's true IP address, however – the Title III order also provided such authority. The Ninth Circuit has held that when the government obtains a Title III order to intercept contents of communications, it may also collect associated non-content information. *See United States v. Kail*, 612 F.2d 443, 448 (9th Cir. 1979). That is what the government did here: it used the NIT to determine the true IP address associated with communications that the government was authorized to intercept pursuant to a Title III order.

In *Kail*, a pre-pen register statute case, the government obtained a wiretap order, but it did not obtain separate authorization for the pen register it installed to collect associated dialed phone number information. As the Ninth Circuit explained, "[b]ecause pen registers do not intercept the contents of communications, they are not within the scope of Title III." *Kail*, 612 F.2d at 448. The court held, however, that obtaining a wiretap order was sufficient authorization for the pen register: "once a valid wiretap order has been issued, as here, there need not be separate authorization for the pen register. . . . If, as defendants argue, the Government must support the use of the pen register by a showing of probable cause that showing is met by satisfying the probable cause requirements for obtaining the wiretap." *Id.*

In this case, the government obtained a Title III order that authorized it to intercept Michaud's communications with "Website A." Ex. 5. Order, p. 2-3. The district court in EDVA had jurisdiction to issue this order, as the order authorized interception of communications with a server located in that district. *See* 18 U.S.C. § 2518(3). The order authorized the government "to intercept electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: . . . the location and identity of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

computers used to further the offenses." *Id*. at 3. Michaud's communications with "Website A" fell within the scope of this authorization.

Thus, under the holding of *Kail* that "once a valid wiretap order has been issued, as here, there need not be separate authorization for the pen register," the Title III order provided appropriate authority for the government to collect non-content information associated with the intercepted communications, including Michaud's true IP address. The Ninth Circuit has held that IP address information in the Internet context is analogous to dialed number information in the telephone context. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007). Although IP address information is typically collected without a warrant at all, *see id.* at 510-511, the government here had authority to collect it both under the Title III order and the Rule 41 warrant. As in *Kail*, "[i]f . . . the Government must support the use of the pen register by a showing of probable cause that showing is met by satisfying the probable cause requirements for obtaining the wiretap." Indeed, the government explained to the issuing district court in its Title III affidavit that it planned to use the NIT to determine the true IP address of website users. *Id.*, Affidavit, p. 31. The government also stated that it planned to obtain additional authorization to use the NIT (which it did), but under *Kail*, additional authorization was not essential. Because the Title III order provided sufficient authority to collect Michaud's true IP address when he accessed "Website A," his motion to suppress should be denied.

Even if Michaud were correct that Rule 41 did not allow the government to obtain a warrant for use of the NIT, and if the Title III order did not provide authorization either, then the use of the NIT would nevertheless still be reasonable under the Fourth Amendment. The Supreme Court has recognized that the presumption that warrantless searches are unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). The Ninth Circuit has defined exigent circumstances as "those circumstances that would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *United States v. Martinez*, 406 F.3d 1160, 1164 (9th Cir. 2005) (quoting *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir.1984) (*en banc*) (abrogated on other grounds)). Courts must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 59 (2013).

Here, if the government could not obtain a warrant for use of the NIT, use of the NIT was justified by exigency. There was a compelling need to use the NIT: "Website A" enabled ongoing sexual abuse and exploitation of children on a massive scale, and use of the NIT was necessary both to stop the abuse and exploitation and to identify and apprehend the abusers. The information it collected was fleeting – if law enforcement had not collected IP address information at the time of user communications with "Website A," then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Accordingly, if the warrant could not be issued, then no warrant could have been obtained in a reasonable amount of time to identify perpetrators. *See United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. An IP address belongs to an ISP, not Michaud, and the Ninth Circuit has held that a defendant lacks a reasonable expectation of privacy in IP addresses. *Forrester*, 512 F.3d at 510. Before proceeding with a more invasive

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

entry and search of Michaud's home and electronic devices, the government obtained a Rule 41 warrant issued in this district.

In sum, the NIT warrant and the Title III order provided authority for use of the NIT, and it is preferable that the government use warrants (as here) to investigate large criminal enterprises like "Website A." Criminals use anonymizing technologies like Tor to perpetrate crimes should not place them beyond the reach of law enforcement (or courts). But even if no court had authority to issue a warrant to deploy a NIT to investigate "Website A" users, its use was nonetheless reasonable under the Fourth Amendment.

C. Suppression is Neither Required Nor Reasonable in this Case

Assuming *arguendo* that the warrant was somehow deficient under Rule 41, suppression is neither required by law nor reasonable under the circumstances. "Rule 41 violations fall into two categories: fundamental errors and mere technical errors." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). "Fundamental errors are those that result in clear constitutional violations." *Id*. By contrast, technical errors may only trigger suppression upon a proper showing of prejudice or "deliberate disregard" for Rule 41. *Id*.[13]

Suppression is a disfavored outcome in this circuit, even in cases presenting constitutional violations. *See, e.g.*, *Negrete-Gonzales*, 966 F.2d at 1283. "[W]e have repeatedly held – and have been instructed by the Supreme Court – that suppression is rarely the proper remedy for a Rule 41 violation." *United States v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006). "Because the exclusionary rule tends to exclude evidence of high reliability, the suppression sanction should only be applied when necessary and not in any automatic manner." *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988) (affirming denial of suppression motion despite a technical violation of Rule 41).

[13] Michaud argues that all three bases apply, though he casts the alleged Rule 41 violations as "of constitutional magnitude" and "not mere technical violations." Mot. at 15, 16. While his argument appears cabined to just presenting a fundamental violation, the Government will respond to all of his arguments for sake of completeness.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Whether exclusion is warranted "must be evaluated realistically and pragmatically on a case-by-case basis." *Id*. (*quoting United States v. Vasser*, 648 F.2d 507, 510 n.2 (9th Cir. 1981), *cert. denied*, 450 U.S. 928 (1981)).

None of the three bases Michaud alleges warrant suppression stand up to scrutiny. He argues that the alleged violation of Rule 41's jurisdictional limitations "is of constitutional magnitude because it did not involve mere ministerial violations of the rule." Mot. at 14. But he offers no credible analysis of how use of the NIT represented a "clear constitutional violation." *See United States v. Johnson*, 660 F.2d 749, 753 (9th Cir. 1981) (requiring a showing that the search was "unconstitutional under traditional fourth amendment standards"). That is because none occurred. The Ninth Circuit has made clear that a "paradigmatic example" of a constitutional violation is where *no* warrant is sought. *Luk*, 859 F.2d at 673 (*citing United States v. Alvarez*, 810 F.2d 879 (9th Cir 1987)). In *Alvarez*, the court reversed the defendant's conviction because the district court did not order suppression after the Government arrested the defendant in a non-public place without a warrant despite having sufficient time to obtain one telephonically pursuant to then-Rule 41(c)(2). 859 F.2d at 882-84. That is clearly not the case here. Also, courts have repeatedly found that "a warrant issued by an unauthorized judge" – which Michaud appears to consider the EDVA magistrate judge to be – is not a fundamental or constitutional violation. *Luk*, 859 F.2d at 673 (*citing United States v. Ritter*, 752 F.2d 435 (9th Cir. 1985), *Johnson*, 660 F.2d 749, *United States v. Comstock*, 805 F.2d 1194 (5th Cir. 1986)).

Furthermore, the search and seizure here complied with the Fourth Amendment. The Fourth Amendment states that search warrants may be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. As the Supreme Court has emphasized, this language "require[s] only three things": a warrant must be issued by a neutral magistrate, it must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

a particular offense," and it must satisfy the particularity requirement. *Dalia*, 441 U.S. at 255. The NIT warrant satisfies these requirements. As described *infra*, the NIT warrant affidavit amply supported the magistrate's finding of probable cause. Ex. 1, pp. 10-23, ¶¶ 6-30. It further described the NIT, how it would be deployed against users who logged into the target website, and the limited, non-content information that would be seized as a result of the NIT's deployment. *Id*. at pp. 23-27, ¶¶ 31-37, Atts. A and B.

The Government's actions here were also reasonable under the circumstances. Law enforcement has a substantial interest in identifying users of a massive website trafficking in child pornography. The court-authorized use of the NIT was driven by the Tor-based technology Michaud and other offenders under investigation used to exploit children, which made it impossible for investigators to know where he was located without first using the NIT. *Id*., p. 23-24, ¶ 31. The individual privacy interests here were extremely limited, due to the minimally invasive nature of the NIT search and its focus on IP address information over which Michaud lacks a reasonable expectation of privacy. *See Forrester*, 512 F.3d 500 (Internet users have no expectation of privacy in the IP addresses of the websites they visit); *see also United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers."). Courts must weigh those privacy interests against "the needs of law enforcement," such as the "need for flexibility that allows police to do their job effectively." *United States v. Martinez-Garcia*, 397 F.3d 1205, 1211 (9th Cir. 2005). The very fact the government sought and obtained a warrant from a neutral magistrate protected Michaud from an unreasonable search and seizure in violation of his constitutional rights. *See Alvarez*, 810 F.2d at 883 (interposing magistrate between law enforcement and target protects against unreasonable searches and seizures). Obtaining that warrant from a magistrate judge in the district where the website was hosted and where users like Michaud went to retrieve information from the website was eminently reasonable, particularly given the lack of available options. Moreover, the magistrate

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

judge did not fail in her duty to impartially evaluate the government's request, nor did the government fail to provide any pertinent information to the magistrate judge. The affidavit, for instance, expressly sought authorization to "cause an activating computer – *wherever located* – to send" certain information to a government-controlled computer, Ex. 1, p. 29, ¶ 46(a)(emphasis added), and it repeatedly noted that a primary purpose of the NIT was to "locate" website users. *Id.*, p. 23-25, ¶¶ 31-32, 34.

Michaud argues that he was prejudiced because, he claims, the search of his computer would not have occurred had the Government limited the NIT to just activating computers located in EDVA. *See* Mot. at 15. The actual import of his prejudice argument is that he believes he had a right to anonymously exploit children without being identified by law enforcement using court-authorized investigative methods. That is not the sort of claimed "prejudice" that should result in suppression. Having used Tor to shield his location from investigators, Michaud should not be permitted to wield it as a weapon against the Government's ability to ask a court to authorize a search to identify him. In any event, as noted *supra*, the government nonetheless could have proceeded with the NIT search without a warrant, due to the exigent circumstances created by Michaud's use of the Tor network to conceal his location and identity.

Even if the government knew the location of activating computers, Michaud still would not have been prejudiced. For instance, had Michaud not concealed his true location, the Government could have obtained a search warrant from a magistrate judge in this district. *See United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (rejecting claim of prejudice where law enforcement officer could have obtained warrant from a separate judicial officer); *Johnson*, 660 F.2d at 753 (same). Michaud's reliance on cases such as *United States v. Krueger* and *United States v. Glover* does not alter this. Those cases involved searches of a residence and a car whose precise physical location were known to be located outside of the magistrates' districts when the warrants were issued. *See Krueger*, 998 F. Supp. 2d 1032, 1034-35 (D. Kan. 2014); *Glover*, 736 F.3d 509, 510 (D.C. Cir. 2013). Appropriate warrants, it stands to reason, could have been

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

obtained from judges in the districts where the residence and car were located. Those courts did not consider the facts before this court – where: (1) the defendant deliberately concealed his location, effectively rendering it impossible to seek process in another district, (2) the search occurred only after the defendant entered the magistrate's district by logging onto a server in that district, and (3) the scope of the search was limited to IP address and basic computer-related information.

Michaud also alleges that suppression is appropriate because agents intentionally and deliberately disregarded Rule 41's jurisdictional limitations. *See* Mot. at 16. But the government's putative violation hardly rises to the level of "bad faith." *Luk*, 859 F.2d at 673 ("suppression is required for nonfundamental violations in bad faith"); *see also Williamson*, 439 F.3d at 1134 ("[o]ther cases have equated 'deliberate and intentional disregard' with 'bad faith.'"). As in *Luk*, the warrant request here was the product of a lengthy investigation by agents who, rather than attempting to avoid compliance with Rule 41, deliberately sought to satisfy the letter of Rule 41 by seeking a warrant in the district with the greatest known connection to the criminal activity. *See* 859 F.3d at 675 (describing investigation). There is no evidence that agents hid critical information from the magistrate judge, or otherwise prevented the magistrate from having all the necessary information. This case is hardly analogous to cases such as *United States v. Gantt*, where the Ninth Circuit affirmed suppression because agents deliberately and without justification failed to provide an individual with a copy of a warrant upon request during a search, in violation of Rule 41(d). 194 F.3d 987, 994-95 (1999). Rather, law enforcement reasonably concluded that under Rule 41, an EDVA judge could issue a warrant to install a NIT on a server in EDVA which would be activated only after individuals, whose true location they deliberatively concealed, voluntarily entered EDVA to access the server. Even if that conclusion was erroneous, such a misapprehension is not equivalent to "bad faith" and does not justify suppressing highly probative evidence that agents used to identify Michaud. *See Williamson*, 439 F.3d at 1134 ("where the agent executing the warrant is unaware of the Rule but acts in good faith in executing

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

what he or she believes to be the Rule, he or she has not acted in deliberate disregard of it; thus suppression is not appropriate").

Finally, even if the warrant was not authorized under Rule 41, the good faith exception applies. *See Leon*, 468 U.S. 897 (1984); *Negrete-Gonzales*, 966 F.2d at 1283 (applying good faith doctrine in the context of a Rule 41 violation). The Supreme Court has made clear that, "the exclusionary rule should not be applied when the officer conducting the search acted in objectively reasonable reliance on a warrant issued by a detached and neutral magistrate," even if that warrant "is subsequently determined to be invalid." *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). The analysis turns on whether there is "an *objectively reasonable* basis for [the agents'] mistaken belief that the warrant was valid." *Negrete-Gonzales*, 966 F.2d at 1283 (emphasis in original). Given the strong nexus between the criminal conduct here and EDVA, and the fact that Michaud and others obscured their true location using Tor, it was entirely reasonable to conclude that a judge in EDVA had authority to issue a valid search warrant under Rule 41. Moreover, once the magistrate signed the warrant after having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Sheppard*, 468 U.S. at 989-90 ("we refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested").

Taken together, suppression here is clearly not warranted given that it is rarely appropriate and requires a careful, fact-specific, and pragmatic evaluation; the compelling need for law enforcement to identify users of this website; Michaud's actions to obscure his criminal activity and location from law enforcement; the review here by a neutral magistrate; and the extensive connections between EDVA and the criminal activity, including the fact that Michaud entered the district to access a child exploitation website.

D. Probable Cause Supported the Issuance of the NIT Search Warrant

The defendant does not challenge whether probable cause existed to issue the NIT warrant. Nor would any such argument be persuasive. The 31-page NIT search warrant

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

affidavit, sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and specialized training and experience investigating the sexual exploitation of children, comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered site users who were utilizing anonymizing technology to expose children to ongoing and pervasive sexual exploitation. Ex. 1, p. 1, ¶ 1.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quotation marks omitted). The task of a judge evaluating a search warrant application "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Probable cause requires "only the probability, and not a prima facie showing, of criminal activity." *Gates*, 462 U.S. at 235. "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'commonsense, practical question,'" for which "[n]either certainty nor a preponderance of the evidence is required." *Gates*, 462 U.S. at 246; *see also United States v. Kelley*, 482 F.3d 1047, 1051-52 (9th Cir. 2007), and *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). Indeed, "[f]inely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision." *Gates*, 462 U.S. at 235. The affidavit clearly established a fair probability that the use of the NIT would collect evidence of a crime.

As the NIT affidavit explained, users who wished to access "Website A" were required to register an account, accept registration terms and create a username and password before they could access the site. Ex. 1, p. 14-15, ¶¶ 12-14. Upon registration,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

all of the sections, forums, and sub-forums were observable. *Id*., p. 15, ¶ 14. The vast majority of those sections were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. *Id*., pp. 15-16, ¶14. The affidavit described, in graphic detail, particular child pornography that was available to all registered users of Website A, that depicted prepubescent females, males and toddlers, being subjected to sexual abuse and exploitation by adults. *Id*., pp. 17-18, ¶ 18. Although the affidavit clearly stated that "the entirety of [Website A was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id*. pp. 20-21, ¶ 27.

It is unlawful to access any computer disk – such as a website's computer server – with the intent to view child pornography, or to attempt to do so. 18 U.S.C. § 2252A(a)(5)(b). Accordingly, among other offenses, any suspect user of "Website A" who accessed the site, or attempted to, with that intent would be guilty of that crime. To that end, the veteran NIT affiant affirmatively articulated that there was "probable cause to believe that . . . any user who successfully accesse[d]" the website had, at a minimum, "knowingly accessed with intent to view child pornography, or attempted to do so." Ex. 1 p. 13, ¶ 10. He made that assessment in light of the "numerous affirmative steps" required for a user to find and access "Website A," which made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content." Ex. 1, p. 12-13, ¶ 10. The Ninth Circuit has repeatedly held that "a magistrate may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found," *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)), including in child pornography cases. *See, e.g., United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The affiant's assessment (and, accordingly, the magistrate's reasonable reliance upon it) was overwhelmingly supported by information articulated within the warrant. "Website A" was no ordinary, run-of-the-mill website that any unknowing person could stumble upon, let alone access. Rather, because the website operated on Tor, a user first had to connect to Tor network and find the site, which required a user to obtain its lengthy, alphanumeric web address. Ex. 1, p. 12, ¶10. That user "might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location" – such as from a Tor "hidden service" page dedicated to pedophilia and child pornography, which contained a section with links to Tor hidden services that contain child pornography – including "Website A". *Id.* Moreover, upon arrival at the site's main page, before logging in, a user saw "to either side of the site name . . . two images depicting partially clothed prepubescent females with their legs spread apart." *Id.* 1, p. 13 ¶ 12. The text underneath those suggestive images of prepubescent girls – "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview" – indicated the site's dedication to image distribution. *Id.* 1, p. 13, ¶ 12.[14] The site's registration terms also contained numerous indications that the site pertained to illicit activity – repeatedly warning prospective users to be vigilant about their security and the potential of being identified. *Id.*, pp. 14-15, ¶ 13. The issuing magistrate could accordingly have reasonably drawn an inference that any user who successfully found "Website A" was aware of its purpose and content.

The full, documented content of the website, as described in the affidavit, made it evident that the site's primary purpose was to advertise and distribute child pornography. Courts have routinely held that membership to a child pornography website, even without specific evidence of suspect downloading child pornography, provides sufficient probable

[14] The affiant articulated that, [b]ased on [his] training and experience, [he] know[s] that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to the site and ".7z" refers to a preferred method of compressing large files or sets of files for distribution." Ex. 1, p. 13, ¶ 12.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

cause for a search warrant because of the commonsense, reasonable inference that someone who has taken the affirmative steps to become a member of such a website would have accessed, received or downloaded images from it. *See Gourde*, 440 F.3d at 1070 (finding sufficient probable cause for residential search where defendant paid for membership in a website that contained adult and child pornography; noting reasonable, common-sense inference that someone who paid for access for two months to a website that purveyed child pornography probably had viewed or downloaded such images onto his computer); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005) (finding probable cause where purpose of the e-group "girls12-16" was to distribute child pornography; noting "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material"); *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted mainly to distributing and collecting child pornography and defendant used suggestive email address); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a [child pornography] group . . . , remains a member of the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession."); *United States v. Hutto*, 84 Fed. Appx 6 (10th Cir. 2003) (affidavit sufficient to show probable cause where defendant became a member of a group whose obvious purpose was to share child pornography, and the images were available to all group members); *but see United States v. Falso*, 544 F.3d 110 (2nd Cir. 2008) (suppressing evidence from residential search for lack of probable cause where defendant was never accused of actually gaining access to the website that contained child pornography, there was no evidence that the primary purpose of the website was collecting and sharing child pornography, and defendant was never said to have ever been

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

a member or subscriber of any child pornography site).[15] Here, like *Gourde*, the reasonable inference that the registered "Website A" users, at a minimum, accessed the site, or attempted to do so, with the intent to view child pornography easily meets the "fair probability" test.

E. The Government Provided Timely Notice of the Search Warrant

Michaud also contends that he was not provided timely notice of the execution of the NIT warrant. He is incorrect. The issuing magistrate authorized delayed notice, which was lawfully extended past the date on which the government provided Michaud with a copy of the warrant.

Rule 41 allows for the delay of any notice required by the rule "if the delay is authorized by statute." Fed R. Crim P. 41(f)(3). The NIT affidavit specifically requested that any notice due to be provided to the person from whom, or from whose premises, property was taken, be delayed pursuant to Fed. R. Crim. P. 41(f)(3) and 18 U.S.C. § 3103a. Ex. 1, pp. 27-28, ¶¶38-41; Warrant App. The Court granted the delayed notice request, checking the box on the warrant to commemorate a finding that "immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial)," and authorizing "the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days." *Id*., Warrant.

Title 18 Section 3013a(c) permits the court to extend delayed notice for good cause shown. On April 3, 2015, June 30, 2015, and September 24, 2015, the U.S. District Court for EDVA granted 90-day extensions of delayed notice. Ex. 4. The September 24, 2015, extension runs until December 23, 2015. The defendant concedes that he was provided a copy of the NIT warrant, through discovery, as of August 19, 2014. Mot. at 17. Accordingly, any notice due was lawfully delayed and timely provided.

---

[15] All of those cases evaluated probable cause before 18 U.S.C. § 2252A(a)(5)(B) was amended to make it unlawful to knowingly access a computer disk with intent to view child pornography, compare 18 U.S.C. § 2252A(a)(5)(B)(effective July 27, 2006) with 18 U.S.C. § 2252A(a)(5)(B)(effective October 8, 2008), making this case even stronger in terms of probable cause.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

III. CONCLUSION

For all the foregoing reasons, the Court should deny Defendant's motion to suppress.

Dated this 16th day of November, 2015.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

s/ S. Kate Vaughan
S. KATE VAUGHAN
Assistant United States Attorney
700 Stewart Street, Suite 5200
Seattle, WA
Phone: (206) 553 7970
Fax: (206) 553 0882
E-mail: kate.vaughan@usdoj.gov

s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 16, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorneys of record for the defendant.

/s/ Rebecca Eaton

LISA CRABTREE
Legal Assistant
United States Attorney's Office
700 Stewart St., Suite 5220
Seattle, Washington 98101
Telephone: (206) 553-5127
Fax: (206) 553-0755
E-mail: rebecca.eaton@usdoj.gov

EXHIBIT

2

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED LODGED
RECEIVED
JUL 09 2015
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY DEPUTY

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

5264 NE 121st Ave, Apartment 150
Vancouver, WA 98682

Case No. MJ15-5111

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The residence at 5264 NE 121st Ave, Apartment 150, Vancouver, WA 98682 as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. § 2252(a)(2)	(receipt and distribution of child pornography)
18 U.S.C. § 2252(a)(4)(B)	(possession of child pornography)

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SAMUEL A. MAUTZ, SPECIAL AGENT, FBI
Printed name and title

Sworn to before me pursuant to Rule 4.1. ~~and signed in my presence.~~

Date: 7/9/2015

Judge's signature

City and state: TACOMA, WASHINGTON

DAVID W. CHRISTEL, U.S. MAGISTRATE JUDGE
Printed name and title

2015R00778

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

INTRODUCTION

I, Samuel A. Mautz, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent of the FBI since 2011, and am currently assigned to the Vancouver, Washington Resident Agency of the Seattle, Washington Division. Previously I was assigned to the Pierre, South Dakota Resident Agency of the Minneapolis, Minnesota Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography. I have gained experience through training at the FBI Academy in Quantico, VA as well as training to be a Digital Extraction Technician for the FBI and everyday work relating to conducting these types of investigations. While assigned to the Pierre, South Dakota Resident Agency, I conducted investigations in conjunction with the South Dakota Internet Crimes Against Children Task Force. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), are located within 5264 NE 121st Ave, Apartment 150, Vancouver, WA 98682 (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachments A and B, incorporated herein by reference, which is located in the Western District of Washington. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation

and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

4. This affidavit in support of the search warrant is being presented electronically because I am located in Vancouver, Washington.

DEFINITIONS

5. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide

the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been

created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to,

central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to

"unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

p. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses

the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

q. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

s. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape

recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

u. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

x. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP");

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. Jay Michaud or a user of the Internet account at 5264 NE 121st Ave, Apartment 150, Vancouver, WA 98682 has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A."[1] There is probable cause to believe that Jay Michaud or a user of the Internet account at 5264 NE 121st Ave, Apartment 150, Vancouver, WA 98682 knowingly accessed with intent to view/receive/distribute child pornography on "Website A."

[1] The actual name of "Website A" is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

The Network[2]

7. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.[3] Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

8. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.[4] Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after

---

[2] The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

[3] Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

[4] Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

9. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

10. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user

can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Description of "Website A" and its Content

11. "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

12. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is

when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

13. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used

to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

14. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

15. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and "scat" refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

16. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post.

The "last post" section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

17. A review of the various topics within the "[Website A] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

18. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

a. On February 3, 2015, a user posted a topic entitled "Buratino-06" in the forum "Pre-teen – Videos - Girls HC" that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

b. On January 30, 2015, a user posted a topic entitled "Sammy" in the forum "Pre-teen – Photos – Girls" that contained hundreds of images depicting child

pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

c. On September 16, 2014, a user posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

19. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, "Website A" contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

20. "Website A" also included a feature referred to as "[Website A] Image Hosting." This feature of "Website A" allowed users of "Website A" to upload links to images of child pornography that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on

"[Website A] Image Hosting." The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

21. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse.

a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

Court Authorized Use of Network Investigative Technique

22. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A

publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

23. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."

24. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information

about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

Summary of Pewter on "Website A"

25. According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT, a user with the user name Pewter engaged in the following activity on "Website A."

26. The profile page of user Pewter indicated this user originally registered an account on "Website A" on October 31, 2014. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user Pewter's profile, this user was a Newbie Member of "Website A." Further, according to the Statistics section of this user's profile, the user Pewter had been actively

logged into the website for a total of 99 hours between the dates of October 31, 2014, and March 2, 2015.

27. User "Pewter" viewed 187 different threads on "Website A" including threads with the titles: "10yo teen with anal front with his father";

"2012, Lolita Cat Goddess 4";

"alicia 10 yo little girl loves adult sex (cum in mouth)";

"7yo APRIL hj bj finger pencil in ass vib cum"; and

"Lauri ~8yo 3 videos, tasting cum".

28. Most of the threads viewed by Pewter included links to view files and comments regarding child pornography. Pewter was observed accessing "Website A" on seven of the ten days during the period of February 21, 2015 through March 2, 2015.

IP Address and Identification of User Pewter on "Website A"

29. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 28, 2015, the user Pewter engaged in the following activity on "Website A" from IP address 73.164.163.63. During the session described below, this user browsed "Website A" after logging into "Website A" with a username and a password.

30. On February 28, 2015, the user Pewter with IP address 73.164.163.63 accessed the post entitled "Girl 12ish eats other girls/dirty talk" in the section "Pre-teen Videos >> Girls HC". Among other things, this post contained a download link to a .html file with the password provided to conduct the download.

31. During the following additional sessions, the user Pewter also browsed "Website A" after logging into "Website A" with a username and password. During these sessions, the user's IP address information was not collected.

32. On March 2, 2015, the user Pewter accessed a post that contained a link to an image that depicted a prepubescent female being anally penetrated by the erect penis of an adult male.

33. On March 2, 2015, the user Pewter accessed a post that contained a link to the same aforementioned image, which depicted a prepubescent female being anally penetrated by the erect penis of an adult male.

34. I have reviewed the images that were accessed by Pewter on March 2, 2015. The images depict a prepubescent female's nude crotch. There is a total lack of pubic and body hair on the female, and the female appears to be prepubuscent in size. The female's legs are spread apart and her vagina is exposed. An adult male's erect penis is penetrating the minor female's anus.

35. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") Comcast.

36. In March 2015, an administrative subpoena/summons was served to Comcast requesting information related to the user who was assigned to the above IP address. According to the information received from Comcast, Jay Michaud was receiving Internet service at 2201 NE 112th Ave., Unit D39, Vancouver, WA 98684, with the same address being listed as the billing address. Internet service was initiated at the

aforementioned premises on October 1, 2014 and was current as of March 9, 2015. The information received from Comcast also listed account number 877810104138548 and telephone number 360-977-8555.

37. A search of the LexisNexis Accurint information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) and other public databases was conducted for Jay Michaud, 2201 NE 112th Ave., Apartment D39, Vancouver, WA 98684. These public records indicated that Jay Michaud's current address is 5264 121st Ave. NE, Apartment 150, Vancouver, WA 98682. The reported date of that address for Michaud was May 8, 2015. These public records also indicated that a previous address for Jay Michaud was 2201 NE 112th Ave., Apartment D39, Vancouver, WA 98684. The latest report date for that address was March 11, 2015.

38. Another search of the LexisNexis Accurint information database was done for 5264 121st Ave. NE, Apartment 150, Vancouver, WA and 2201 NE 112th Ave., Apartment D39, Vancouver, WA. That search indicated that during the times that those addresses were occupied by Jay Michaud, there were no other listed occupants at those addresses.

39. In June of 2015, another administrative subpoena was served to Comcast requesting information related to the account of Jay Michaud with account number 8778101014138548. According to the information received from Comcast, that account had been disconnected as of May 8, 2015. The information received from Comcast

indicated that account number 8778101014138548 associated with Jay Michaud had been transferred to a new account with subscriber name Jay Michaud with subscriber address 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682.

40. On June 16, 2015, I reviewed the Clark County Public Utilities database. The database indicated that services are being provided to Jay Michaud at 5264 NE 121st Ave., Apartment Q150, Vancouver, WA 98682 with home telephone number 390-977-8555, and services start date of May 8, 2015.

41. In June of 2015, a third administrative subpoena was served to Comcast requesting information related to the account of Jay Michaud at 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682. According to the information received from Comcast, Jay Michaud was receiving Internet service at 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682. Internet service was initiated at the aforementioned premises on May 8, 2015, and was current as of June 23, 2015. The information received from Comcast also listed telephone number 360-977-8555.

42. I have conducted surveillance at the TARGET PREMISES. On July 7, 2015, I noted that a Nissan Altima with Washington Plate ARL3559 was parked in the parking lot near the TARGET PREMISES. A vehicle registration check was conducted for Washington Plate ARL3559 and that license came back to a 2008 Nissan Altima registered to Jay E. Michaud at 2201 NE 112th Ave., Apt D39, Vancouver, WA.

43. I have reviewed Washington State Employment records showing that from the 4th Quarter of 2013 through the 1st Quarter of 2015, Jay Michaud was employed with the

Vancouver School District 37. I have also reviewed information on the website data.kitsapsun.com, which maintains a database for teachers' salaries and teaching experience in the state of Washington. The site, data.kitsapsun.com, shows Jay Michaud as an employee of the Vancouver School District with 11 years of certified experience. I have reviewed the staff directory of Gaiser Middle School as reflected on their website. Gaiser Middle School is a middle school in the Vancouver School District. The staff directory reflects that Jay Michaud is a part of the Special Education Department at Gaiser Middle School.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW AND/OR COLLECT, RECEIVE, OR DISTRIBUTE CHILD PORNOGRAPHY

44. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view and/or possess, collect, receive or distribute images of child pornography:

a. Individuals who access with intent to view and/or possess, collect, receive or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who access with intent to view and/or possess, collect, receive or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who access with intent to view and/or possess, collect, receive or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who access with intent to view and/or possess, collect, receive or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a

computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who access with intent to and/or possess, collect, receive or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who access with intent to view and/or possess, collect, receive or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law

enforcement officers involved in the investigation of child pornography throughout the world.

45. Based on the following, I believe that a user of the Internet account at SUBJECT PREMISES, likely displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography. For example, the user :

a. Began accessing "Website A" on October 31, 2014 and continued to access "Website A" through March 2, 2015.

b. Spent a total amount of over 99 hours logged on to "Website A"

c. Viewed 187 different threads on "Website A" including threads with the titles, "10yo teen with anal front with his father", "2012, Lolita Cat Goddess 4, alicia 10 yo little girl loves adult sex (cum in mouth)", "7yo APRIL hj bj finger pencil in ass vib cum" and "Lauri ~8yo 3 videos, tasting cum".

d. Was observed on "Website A" on seven of the ten days during the period of February 21, 2015 through March 2, 2015.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

46. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

47. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

48. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service,

chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

49. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

50. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

51. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety

of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

52. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

53. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled

environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronically stored information ("ESI") is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to

two terabytes (2,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

54. In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Attachment B. Further, the government anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child pornography image files. Use of these tools will allow for the quick identification of

evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case.

55. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of

items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

56. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

Instrumentalities

57. Based on the information in this Affidavit, I also believe that the digital device(s) at the SUBJECT PREMISES are instrumentalities of crime and constitute the means by

which violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) have been committed. Therefore, I believe that in addition to seizing the digital devices to conduct a search of their contents as set forth herein, there is probable cause to seize those digital devices as instrumentalities of criminal activity.

Conclusion

58. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

Special Agent Samuel A. Mautz
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 9th *day of* July, *20*15.

DAVID W. CHRISTEL
Magistrate Judge

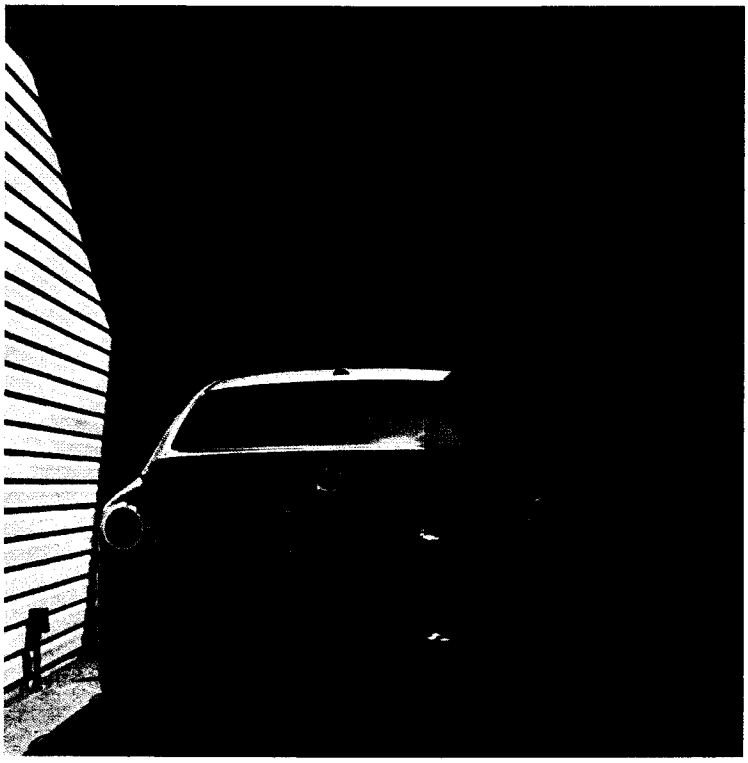
ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 5264 NE 121st Ave, Apt 150, Vancouver, WA 98682 is identified as follows: an apartment located in the building labeled "Q" in the One Lake Place apartment complex. Apartment 150 is accessed from the stairwell in the middle of building "Q". Apartment 150 is on the third floor and is the doorway to the right or south at the top of the stairs.

The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES of 5264 NE 121st Ave, Apt 150, Vancouver, WA 98682 including any storage units/outbuildings or garages and 2008 Nissan Altima with Washington License Plate ARL 3559. The vehicle described has been seen parked near SUBJECT PREMISES and is registered to Jay Michaud at Michaud's previous residence address. Jay Michaud has moved primary residence in the past three months and would likely have used his vehicle to transport items from his previous residence to his current residence. Digital media and items to be described in Attachment B could also be easily stored and concealed in a vehicle.

PICTURE



ATTACHMENT B

Information to be Seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251 and 2252:

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including

   a. Records, information, and items relating to the occupancy or ownership of 5264 NE 121st Ave, Apt 150, Vancouver, WA 98682 including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

   b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

   c. Records and information relating to sexual exploitation of children, including correspondence and communications between users of Website A.

Search Protocol

In accordance with the information in the Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of this Attachment B. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data

contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to this Attachment B.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

EXHIBIT

3

EXHIBIT 3

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

FILED LODGED
RECEIVED
AUG 11 2015
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
LG cellular smart phone, S/N 210KPFX015875

Case No. MJ15-5136

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
The LG cellular smart phone, S/N 210KPFX015875 as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. §§ 2252(a)(2) and 2252 (a)(4)(B)	receipt and distribution of child pornography; possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SAMUEL A. MAUTZ, SPECIAL AGENT, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: August 11, 2015

Judge's signature

City and state: Tacoma, Washington

KAREN L. STROMBOM, U.S. MAGISTRATE JUDGE
Printed name and title

2015R00778

AFFIDAVIT

STATE OF WASHINGTON)
)
COUNTY OF CLARK)

I, Samuel A. Mautz, having been duly sworn, state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2011, and am currently assigned to the Vancouver, Washington Resident Agency of the Seattle, Washington Division. Previously I was assigned to the Pierre, South Dakota Resident Agency of the Minneapolis, Minnesota Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography. I have gained experience through training at the FBI Academy in Quantico, VA as well as training to be a Digital Extraction Technician for the FBI and everyday work relating to conducting these types of investigations. While assigned to the Pierre, South Dakota Resident Agency, I conducted investigations in conjunction with the South Dakota Internet Crimes Against Children Task Force. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. The statements contained in this affidavit are based in part on information provided by law enforcement officials and others known to me, and on my experience and background as a law enforcement officer. Since the affidavit is being submitted for

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18, United States Code, §§ 2252(a)(2) and 2252 (a)(4)(B), have been committed and that the instrumentalities, fruits, and evidence of those crimes will be found in a particular place to be searched.

3. This affidavit is made in support of a search warrant for the following item, which is currently in the legal custody of Vancouver Police Department – an LG cellular smart phone, S/N 210KPFX015875, hereinafter the "SUBJECT DEVICE").

4. The device listed above was seized from the person of JAY MICHAUD on July 10, 2015, and is currently stored in the Vancouver Police Department Seized Property Room, located in Vancouver, Washington.

5. I am submitting this affidavit in support of a search warrant authorizing a search of the SUBJECT DEVICE and the extraction from the SUBJECT DEVICE of electronically stored content and information described in Attachment B hereto, which content and information constitute instrumentalities, fruits, and evidence of the foregoing violations.

6. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

7. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. This affidavit in support of the search warrant is being presented electronically because I am located in Vancouver, Washington.

II. BACKGROUND TO INVESTIGATION

9. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application. Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

10. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet. Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

11. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

12. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

13. According to data obtained from logs on "Website A," a user with the user name Pewter engaged in the following activity on "Website A." The profile page of user Pewter indicated this user originally registered an account on "Website A" on October 31, 2014. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user Pewter's profile, this user was a "Newbie Member" of "Website A." Further, according to the Statistics section of this user's profile, the user Pewter had been actively logged into the website for a total of 99 hours between the dates of October 31, 2014, and March 2, 2015. Pewter viewed 187 different threads on "Website A" including threads with the titles, "10yo teen with anal

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

front with his father", "2012, Lolita Cat Goddess 4, alicia 10 yo little girl loves adult sex (cum in mouth)", "7yo APRIL hj bj finger pencil in ass vib cum" and "Lauri ~8yo 3 videos, tasting cum". Most of the threads viewed by Pewter included links to view files and comments regarding child pornography. Pewter was observed accessing "Website A" on seven of the ten days during the period of February 21, 2015 through March 2, 2015.

14. According to data obtained from logs on "Website A," on February 28, 2015, the user Pewter engaged in the following activity on "Website A" which further law enforcement investigation determined was from IP address 73.164.163.63. During the session described below, this user browsed "Website A" after logging into "Website A" with a username and a password.

15. On February 28, 2015, the user Pewter accessed the post entitled "Girl 12ish eats other girls/dirty talk" in the section "Pre-teen Videos >> Girls HC". Among other things, this post contained a download link to an .html file with the password provided to conduct the download.

16. During the following additional sessions, the user Pewter also browsed "Website A" after logging into "Website A" with a username and password. During these sessions, the user's IP address information was not collected.

> On March 2, 2015, the user Pewter accessed a post that contained a link to an image that depicted a prepubescent female being anally penetrated by the erect penis of an adult male.
>
> On March 2, 2015, the user Pewter accessed a post that contained a link to the same aforementioned image, which depicted a prepubescent female being anally penetrated by the erect penis of an adult male.

17. I have reviewed the images that were accessed by Pewter on March 2, 2015. The images depict a prepubescent female's nude crotch. The female's legs are spread apart and her vagina is exposed. An adult male's erect penis is penetrating the female's anus.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. Using publicly available websites, FBI Special Agents were able to determine that the IP Address associated with this activity was operated by the Internet Service Provider ("ISP") Comcast. In March 2015, an administrative subpoena/summons was served to Comcast requesting information related to the user who was assigned to the above IP address. According to the information received from Comcast, JAY MICHAUD was receiving Internet service at 2201 NE 112th Ave., Unit D39, Vancouver, WA 98684, with the same address being listed as the billing address. Internet service was initiated at the aforementioned premises on October 1, 2014 and was current as of March 9, 2015. The information received from Comcast also listed account number 877810104138548 and telephone number 360-977-8555.

19. A search of the LexisNexis Accurint information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) and other public databases was conducted for JAY MICHAUD, 2201 NE 112th Ave., Apartment D39, Vancouver, WA 98684. These public records indicated that Jay Michaud's current address is 5264 121st Ave. NE, Apartment 150, Vancouver, WA 98682. The reported date of that address for Michaud was May 8, 2015. These public records also indicated that a previous address for Jay Michaud was 2201 NE 112th Ave., Apartment D39, Vancouver, WA 98684. The latest report date for that address was March 11, 2015.

20. Another search of the LexisNexis Accurint information database was done for 5264 121st Ave. NE, Apartment 150, Vancouver, WA and 2201 NE 112th Ave., Apartment D39, Vancouver, WA. That search indicated that during the times that those addresses were occupied by JAY MICHAUD, there were no other listed occupants at those addresses.

21. In June of 2015, another administrative subpoena was served to Comcast requesting information related to the account of Jay Michaud with account number 8778101014138548. According to the information received from Comcast, that account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

had been disconnected as of May 8, 2015. The information received from Comcast indicated that account number 8778101014138548 associated with JAY MICHAUD had been transferred to a new account with subscriber name Jay Michaud with subscriber address 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682.

22. In June of 2015, a third administrative subpoena was served to Comcast requesting information related to the account of Jay Michaud at 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682. According to the information received from Comcast, JAY MICHAUD was receiving Internet service at 5264 NE 121st Ave., Apartment 150, Vancouver, WA 98682. Internet service was initiated at the aforementioned premises on May 8, 2015, and was current as of June 23, 2015. The information received from Comcast also listed telephone number 360-977-8555.

23. I have reviewed Washington State Employment records showing that from the 4th Quarter of 2013 through the 1st Quarter of 2015, JAY MICHAUD was employed with the Vancouver School District 37.

24. On July 9, 2015, I obtained a federal search warrant for the residence located at 5264 NE 121st Ave, Apartment 150, Vancouver, WA. That search warrant was executed by federal agents on July 10, 2015. During the execution of that search a thumb drive was located in the USB port of a TV located in the residence. The thumb drive is a SanDisk Ultra USB 3.0 32 Gigabyte thumb drive. The thumb drive is labeled as being made in China.

25. The thumb drive was reviewed by forensic examiner Eric Thomas of the Vancouver Police Department Digital Evidence and Crimes Unit (DECU). During his review Thomas was able to locate and identify multiple images that are child pornography.

26. I have reviewed three of the images that were previously identified by DECU Forensic Examiner Eric Thomas. All three of the images were located in a folder

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

located on the thumb drive with the folder title "Downloads/Nude". The images I reviewed are described as follows:

> The first image depicts a female child's anus and vagina. The child appears to be an infant based on her relative size and lack of body or pubic hair. There is an adult hand on the infant's right buttock and there is an adult erect penis penetrating the infant's anus.
>
> The second image appears to have been made using night vision and depicts a nude male child lying on his back. The child appears to be of infant or toddler age based on his relative size, lack of body hair and undeveloped penis. There is an adult penis penetrating the child's anus.
>
> The third image depicts a female child lying flat on her back. The child appears to be prepubescent based on her relative size and total lack of body or pubic hair. The child is not wearing pants and her shirt is pulled up to her chest, covering her breasts. There is an adult penis penetrating the child's vagina.

27. On July 10, 2015, at approximately 9:25 a.m., VPD Sgt. Joseph Graaff and Det. Jason Mills followed JAY MICHAUD to Starbucks located at 11211 NE Fourth Plain Blvd., Vancouver, WA 98662. When JAY MICHAUD exited his vehicle, Sgt. Graaff and Det. Mills contacted JAY MICHAUD, greeted and identified him, identified themselves as law enforcement and advised JAY MICHAUD he was being detained based upon their involvement in a child pornography investigation. Sgt. Graaff conducted a search of JAY MICHAUD for officer safety, and in doing so, retrieved a cellular telephone ("LG", S/N 210KPFX015875) from JAY MICHAUD's front right short's pocket. Sgt. Graaff immediately handed the cell phone to Det. Mills, who placed the phone in "airplane mode."

28. At approximately 9:50 a.m., I and SA Adrianne Carrier arrived at the Starbucks. I took possession of the cellular telephone, and advised JAY MICHAUD of the existence of a federal search warrant for JAY MICHAUD's residence.

29. The cellular telephone was entered into FBI evidence control under a separate evidence log than the items seized from the residence/garage.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

30. I subsequently provided the cellular telephone found on JAY MICHAUD to Vancouver Police Department for processing once legal authority is obtained.

31. On August 10, 2015, I spoke with DECU Forensic Examiner (FE) Eric Thomas. FE Thomas reported to me the results of his forensic analysis to date of the thumb drive found in JAY MICHAUD's residence. FE Thomas identified over 70,000 images on the thumb drive. Of those 70,000 images, over 47,000 images were classified as child model or child erotica images, over 24,000 images were pornographic images containing subjects whose age could not be confidently determined, over 2,400 images were classified as child pornography. The thumb drive contained one video containing child pornography. FE Thomas also found 20 page manual entitled, "The Jazz Guide: How to Have Sex With Very Young Girls…Safely." FE Thomas reported he has yet to complete an analysis on the second thumb drive that was seized during the execution of the search warrant on July 10, 2015.

IV. TECHNICAL BACKGROUND

32. I know, based on my training and experience, that cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smart phone on their person; recent investigations in this District have resulted in the discovery of child pornography files on smart phones which were carried on an individual's person at the time the phones were seized. The SUBJECT DEVICE is a smartphone capable of accessing the internet.

33. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the distributor's/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

34. A smartphone's capability to store images in digital form makes it an ideal repository for child pornography. Smartphones can store hundreds of images. It is also possible to use the video camera function on the smartphone to capture an image and save that image to the smartphone.

35. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

collections are often maintained for several years and are kept close by, usually at the individual's residence or on their person, to enable the collector to view the collection, which is valued highly.

d. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

36. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on smartphones. I also know that electronic evidence can be moved easily from one digital device to another.

37. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

38. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of smartphones, I believe that for the SUBJECT DEVICE, there is probable cause to believe that the items set forth in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices including smartphones contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files.

39. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

40. If, after conducting its examination, law enforcement personnel determine that the SUBJECT DEVICE is an instrumentality of the criminal offenses referenced

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that the device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

V. CONCLUSION

29. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are stored on the SUBJECT DEVICE. I therefore request that the court issue a warrant authorizing a search of the listed SUBJECT DEVICE for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

Dated this 11th day of August, 2015.

Samuel Mautz
Special Agent
Federal Bureau of Investigation

The above-named agent provided this sworn statement attesting to the truth of the contents of the foregoing affidavit on 11th day of August, 2015.

KAREN L. STROMBOM
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

The following SUBJECT DEVICE:

An LG cellular smart phone, S/N 210KPFX015875

which is currently stored in the Vancouver Police Department Seized Property Room, located in Vancouver, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

The following SUBJECT DEVICE:

an LG cellular smart phone, S/N 210KPFX015875

which is currently stored in the Vancouver Police Department Seized Property Room, located in Vancouver, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT DEVICE:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

3. All images or records regarding invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

5. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

6. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

7. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

8. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

9. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

11. Evidence of times the digital device(s) was used;

12. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

13. Any evidence of access to Website A, the Network, or communications between individuals regarding Website A or the Network.

SEARCH PROTOCOL

The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to this Attachment B.

If, after conducting its examination, law enforcement personnel determine that the SUBJECT DEVICE is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that the device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT 3

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
LG cellular smart phone, S/N 210KPFX015875

Case No. MJ15-5136

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington
(identify the person or describe the property to be searched and give its location):

The LG cellular smart phone, S/N 210KPFX015875 as further described in Attachment A, which is attached hereto and incorporated herein by this reference, located at vanocuver PD, in vancouver, Washington.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

YOU ARE COMMANDED to execute this warrant on or before August 25, 2015 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: August 11, 2015 @ 10:30 am

Karen L Strombom
Judge's signature

City and state: Tacoma, Washington

KAREN L. STROMBOM, U.S. MAGISTRATE JUDGE
Printed name and title

2015R00778

EXHIBIT 3

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

2015R00778